REMARKS

Claims 33-46 were pending in this application prior to the Office Action. By this amendment, claims 33 and 43 are amended, and new system claims 47-61 are added. No new matter has been added. Thus, claims 33-61 are now pending. Support for the amendments and the new claims can be found throughout the specification, for example, in paragraphs [0066] – [0076] of the published application. In view of the following remarks, reconsideration and allowance of the application is respectfully requested.

Claims 43 stands rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. However, Applicants submit that this rejection should be reconsidered and withdrawn in view of the amendments to claim 43 herein.

Claims 33-46 stand rejected 35 U.S.C. § 103(a) as unpatentable over Sharma et al. (2002/0068559) in view of Albert et al. (2003/0177389), in further view of Nordstrom et al. (7,136,907). However, contrary to the assertions of the Examiner, none of Sharma, Albert, or Nordstrom, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 33-46.

For example, claim 33 recites a method for managing a computer system on a network, the computer system including a computing node located on the network side of a network connection on the network and one or more mobile devices located on a user's side of the network connection on the network. The method comprises *detecting, using a discovery program, one or more mobile devices or resources on the network that are connected to the computing node, detecting, using a discovery program, one or more mobile devices or resources on the network that were previously, but are not currently, connected to the computing node*, determining information regarding at least one of the detected mobile devices or resources based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile

device or resource, and using the determined mobile device information to manage security of the computer system from the network side of the network connection.

Thus, claim 33 provides, in relevant part, steps of detecting, using a discovery program, 1) one or more mobile devices or resources on the network that are connected to the computing node, and 2) one or more mobile devices or resources on the network that were previously, but are not currently, connected to the computing node.

In contrast, Sharma discloses, for example, in paragraph [0066], the use of a basic "network discovery function" which merely browses the network to discover the existing network topology. In particular, Sharma discloses, in paragraph [0062], the use of a network discovery function. As is disclosed in paragraph [0066], the NMS 400 network discovery function is carried out by the network discovery process 426. The network discovery process 426 communicates with the network via the I/O interface 402 to browse the network to discover the existing network topology. The network topology preferably serves as a schematic or blueprint of the assets present on the network, and may include the NMS. The network discovery process 426 forwards the discovered network topology to the view database 424. The view database 424 stores the network topology as well as network topology views 422 associated with the network topology as described below. The view database 424 is a repository of network topology views 422, including PAN and WAN views of the network.

Furthermore, Albert discloses, in paragraph [0024], a system for regulating access at a computing system or device as required for connection of a device to a network. Upon receipt of a request for connection to a network, the connection manager determines access or security rules which are required to allow connection of the device to the network. The rules engine automatically generates a current access policy for regulating access at the computing device as required for connection to a network. The security enforcement module applies this current access policy for regulating access at the computing device.

As admitted by the Examiner, both Sharma and Albert fail to disclose "detecting mobile devices or resources previously, but not currently, connected to the network connection" as was previously recited in the claims. In view of the current claims presented herein, Applicants submit that both Sharma and Albert fail to disclose "detecting, using a discovery program, one or more mobile devices or resources on the network that were previously, but are not currently, connected to the computing node."

In an attempt to overcome this deficiency, the Examiner applies Nordstrom, and states that Nordstrom discloses "a system for dynamically informing an operating system of a distributed computer system, when a (new) device is added on the network" and that Nordstrom discloses that the system is capable of "discovering a device that has been previously connected to the network." However, contrary to the Examiner's assertions, Applicants respectfully submit that Nordstrom also fails to disclose, suggest, or render obvious at least the feature of "detecting, using a discovery program, one or more mobile devices or resources on the network that were previously, but are not currently, connected to the computing node."

Generally, Nordstrom discloses, in col. 2, lines 61-67, a discovery utility that allows an operating system (OS) of a distributed computer system, such as a system area network (SAN), to be notified whenever a new component (node or device) is added to the SAN. The invention is also applicable to *discovery of previously connected devices that were in the OS database but have been removed from the network for one reason or another*. Thus, according to Nordstrom, the discovery of "previously connected devices" relates to devices that "have been removed from the network."

In contrast to the above teachings, the present claims provide a discovery program is used to 1) detect mobile devices or resources on the network that are connected to the computing node, and 2) detect mobile devices or resources on the network that were previously, but are not currently, connected to the computing node.

For example, the Exmainer's attention is directed to paragraphs [0067]-[0076] of the published application, which supports the present claims. In particular, the discovery process can detect and track, how a mobile device or external resource is used and on which systems a particular resource or mobile device has synchronized data. The discovery process can also detect one or more mobile devices or other resources that at one time or another have attached to the system, or foreign and unknown devices (that have not been attached to the network earlier) entering a wired or wireless network of an organization. Thus, the discovery method of the present invention can also discover and secure storage media or any other resource that attach to the computing node or mobile devices. The discovery program can scans domains or computing nodes to detect mobile devices, e.g., based on a domain identity. A scan profile can be used to define the parameters for connecting to domains, computing nodes and mobile devices.

In addition, network management parameters, such as those defined by the Simple Network Management Protocol (SNMP) can be used to locate, detect and discover the types of the mobile devices or resources that have attached to the computing node. Also, the data and packet format as well as associated transport and network protocol parameters, e.g., TCP, UDP, and IP can be used to locate, detect or discover the type of mobile devices. Such mobile device type information is used for managing security in the computer network. By processing any of the gathered information, the discovery system and method of the present invention provides an, effective management tool for managing all security aspects of any computer system.

Therefore, for at least the above reasons, none of Sharma, Albert, or Nordstrom, taken alone or in combination, disclose, suggest, or render unpatentable the invention recited in claims 33-46 under 35 U.S.C. § 103(a). Therefore, Applicants respectfully submit that the rejection of claims 33-46 under 35 U.S.C. § 103(a) should be reconsidered and withdrawn. In addition, new system claims 47-61 correspond to method claims 33-46, and are likewise allowable.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the

undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Except for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a CONSTRUCTIVE PETITION FOR EXTENSION OF TIME in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

NIXON PEABODY, LLP

Date: February 28, 2008

/Stephen M. Hertzler, Reg. No. 58,247/
Stephen M. Hertzler

NIXON PEABODY LLP
Customer No. 22204
401 9th Street, N.W., Suite 900
Washington, D.C. 20004
(202) 585-8000